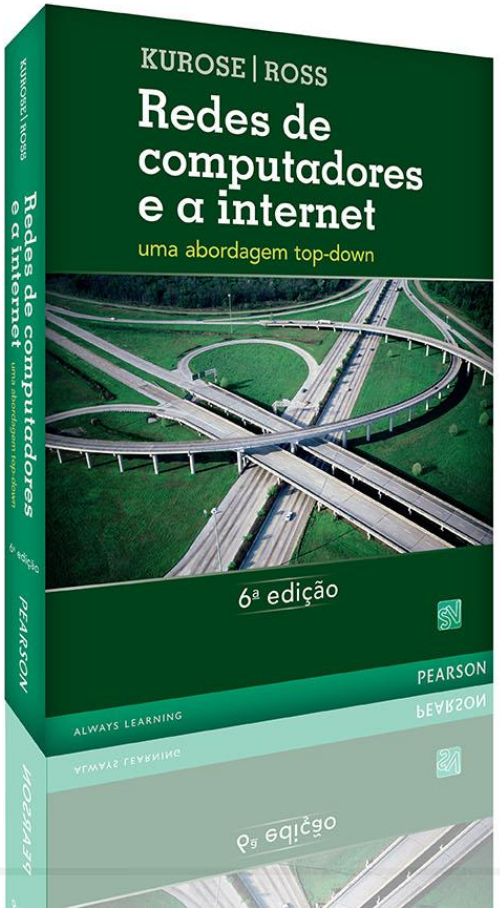
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIADO RIO GRANDE DO NORTE – IFRN
Disciplina: Arquitetura de redes de computadores e Tecnologia de Implementação de Redes
Professor: M Sc. Rodrigo Ronner T. da Silva
E-mail: rodrigo.tertulino@ifrn.edu.br

Capítulo 6

Redes sem fio e redes móveis



Introdução

- Redes de computador em que os meios de transmissão não usam cabos físicos
- Usadas em ocasiões ou locais em que as soluções cabeadas não são empregadas
  - Complementam as redes cabeadas
- Motivação: telefones celulares
- Exemplos comuns
  - Infravermelho
  - Bluetooth
  - Wi-Fi
  - WiMAX

Introdução

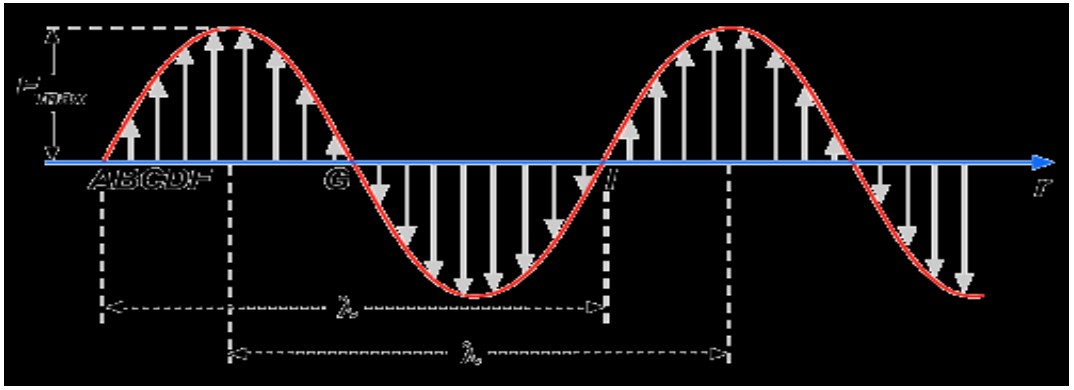
- Flexibilidade e mobilidade
- Convenientes na instalação – evita o trabalho de passagem de cabos
  - Reduz custo (dispensa cabeamento)
- Baratas – Equipamentos tem preço acessível
- Pode ser implementada em praticamente qualquer lugar
- Manutenção reduzida

Introdução

- Largura de banda inferior aos métodos cabeados (Fast e Giga Ethernet)
- Problemas com a segurança da informação
- Qualidade de serviço
  - Força do sinal é decrescente
  - Interferências de outras fontes
  - Propagação multidirecional
- Ligações mais difíceis de estabelecer
  - Necessidade de prot. de correção de erros robusta
  - Partilha do meio de transmissão

Introdução

- Ondas eletromagnéticas são ondas cíclicas que se repetem em uma determinada frequência
  - 1 Hz = 1 ciclo por segundo
  - KHz; MHz; GHz
- Viajam à velocidade da luz
- Comprimento de onda diminui quando a frequência aumenta



Introdução – Padrões WIFI

- *Wireless Fidelity* – Nome comercial dado à família de padrões 802.11 do IEEE
- Disseminação muito grande nos últimos anos
  - Notebooks e PDAs normalmente já suportam o uso nativamente
- Padrões comerciais
  - 802.11a (5 GHz; 54 Mbps) FHSS ou DSSS, modulação BPSK – Largura 20 Mhz
  - 802.11b (2.4 GHz; 11 Mbps) DSSS, modulação BPSK/QPSK – Largura 22 Mhz
  - 802.11g (2.4 GHz; 54Mbps) OFDM (52 subportadoras), modulação QAM64 - Largura 20 Mhz
  - 802.11n (2.4/5 GHz; 300Mbps) OFDM (108 subportadoras), modulação QAM64, MIMO 4x4 - Largura 20/40 Mhz
  - 802.11ac (5 GHz; 1,3 Gb/s) OFDM (234, 2x234 subportadoras), modulação QAM256, MIMO 8x8 - Largura 80/160 Mhz

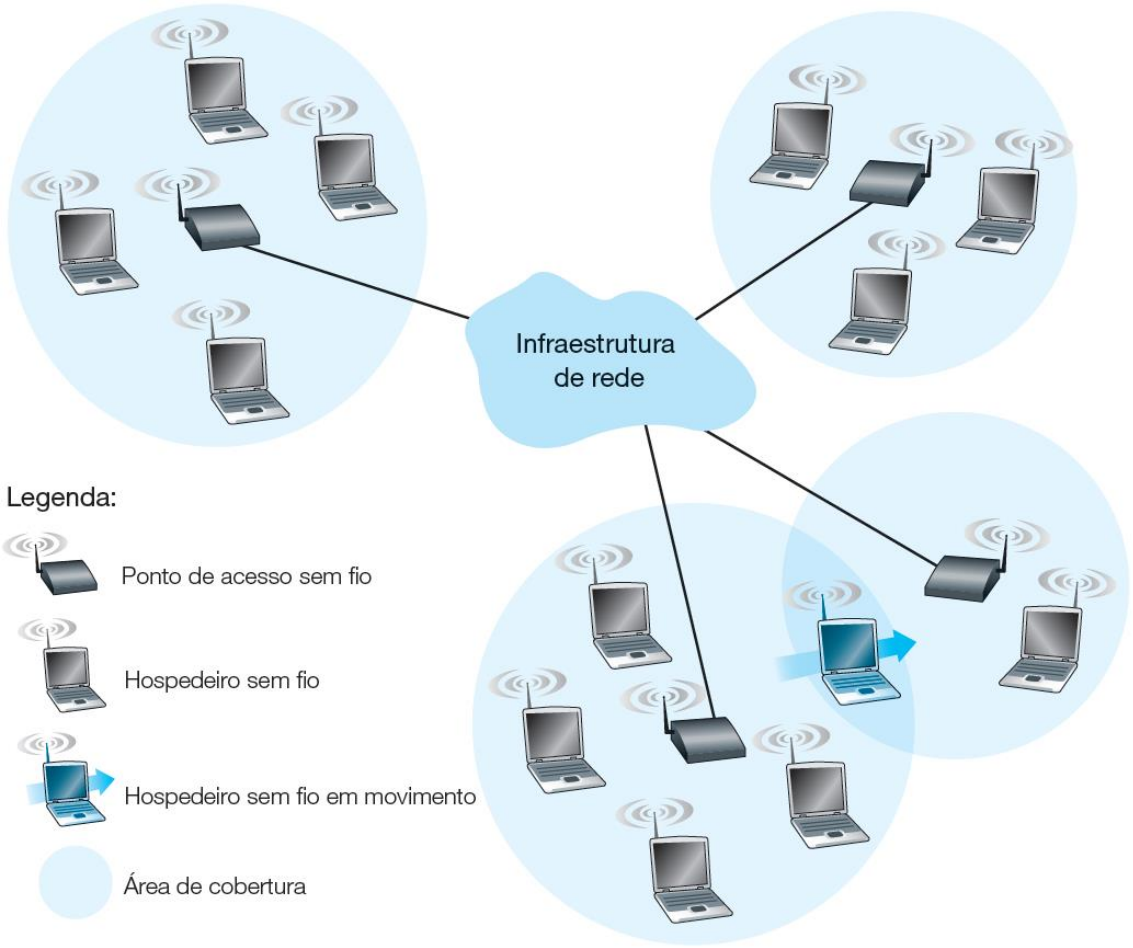
Introdução

Podemos identificar os seguintes elementos em uma rede sem fio:

- Hospedeiros sem fio.
- Enlaces sem fio.
- Estação-base.
- Infraestrutura de rede.

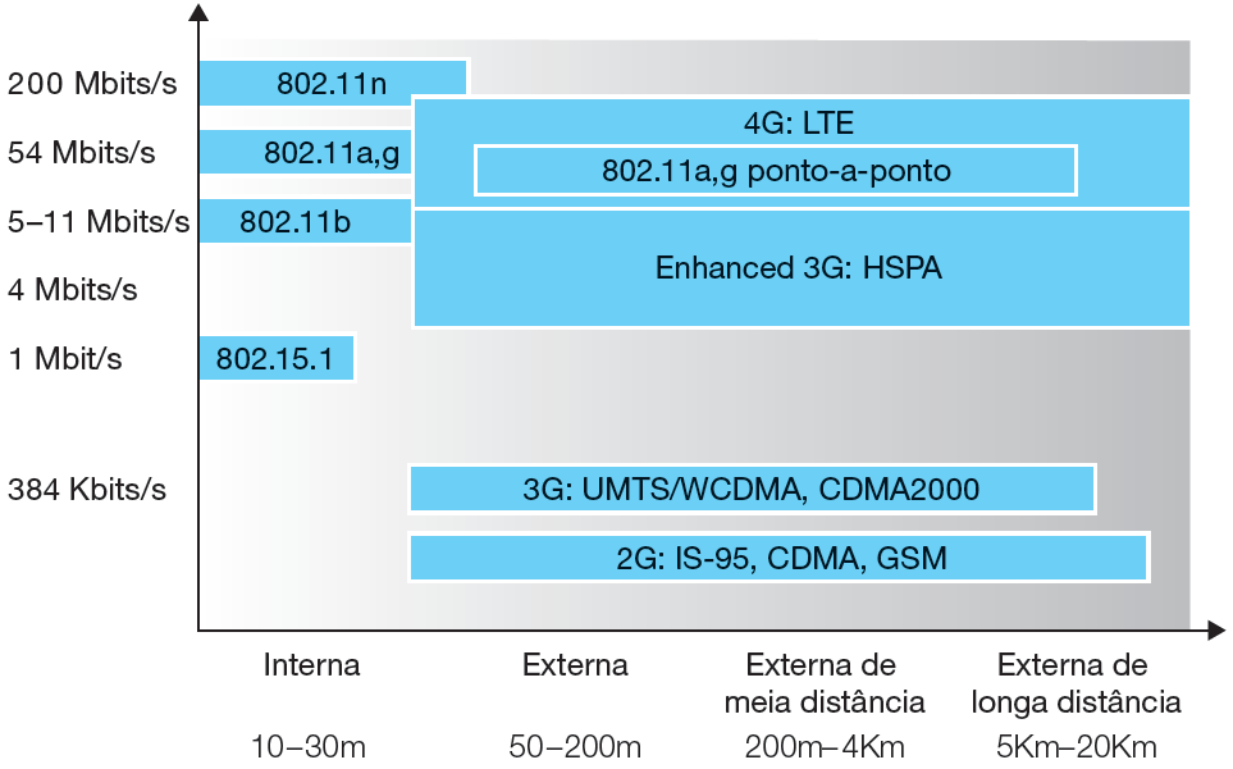
Introdução

- Elementos de uma rede sem fio



Introdução

- Características de enlaces de padrões selecionados de rede sem fio



Características de enlaces e redes sem fio

Podemos encontrar várias diferenças importantes entre um enlace com fio e um enlace sem fio:

- Redução da força do sinal.
- Interferência de outras fontes.
- Propagação multivias.

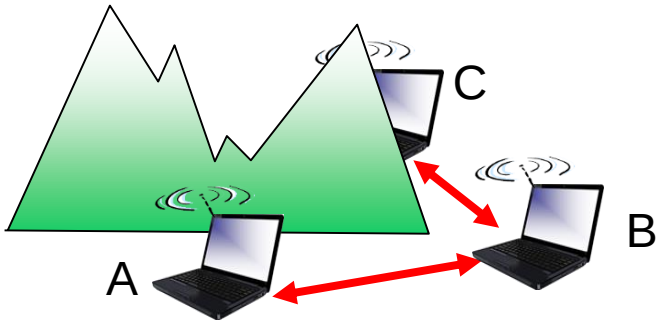
Wi-Fi: LANs sem fio 802.11

- A LAN sem fio 802.11b tem uma taxa de dados de 11 Mbits/s e opera na faixa de frequência não licenciada de 2,4 a 2,485 GHz.

- A distância de transmissão dessas LANs é mais curta para determinado nível de potência e elas sofrem mais com a propagação multivias.

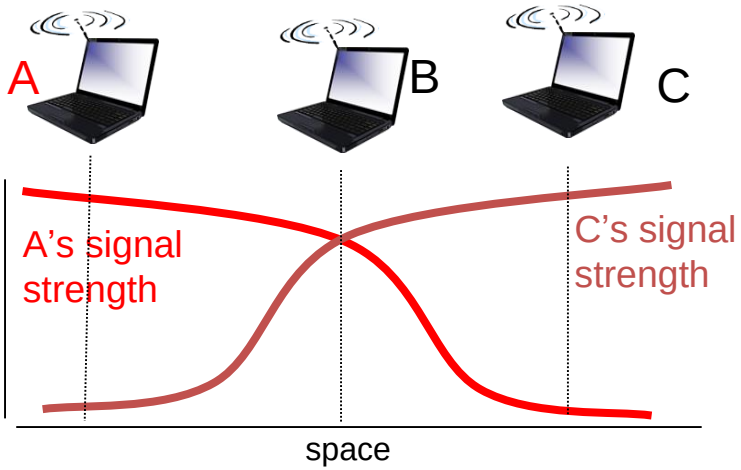
- Um padrão Wi-Fi relativamente novo, 802.11n [IEEE 802.11n, 2012], utiliza duas ou mais antenas no lado remetente e duas ou mais antenas no lado destinatário que estão transmitindo/recebendo sinais diferentes.

Características de enlaces e redes sem fio



Problema do Terminal Oculto

- B, A ouvir um ao outro
- B, C ouvir um ao outro
- A, C não podem ouvir um ao outro, significa que A, C escutem transmissões um do outro, interferindo em B.

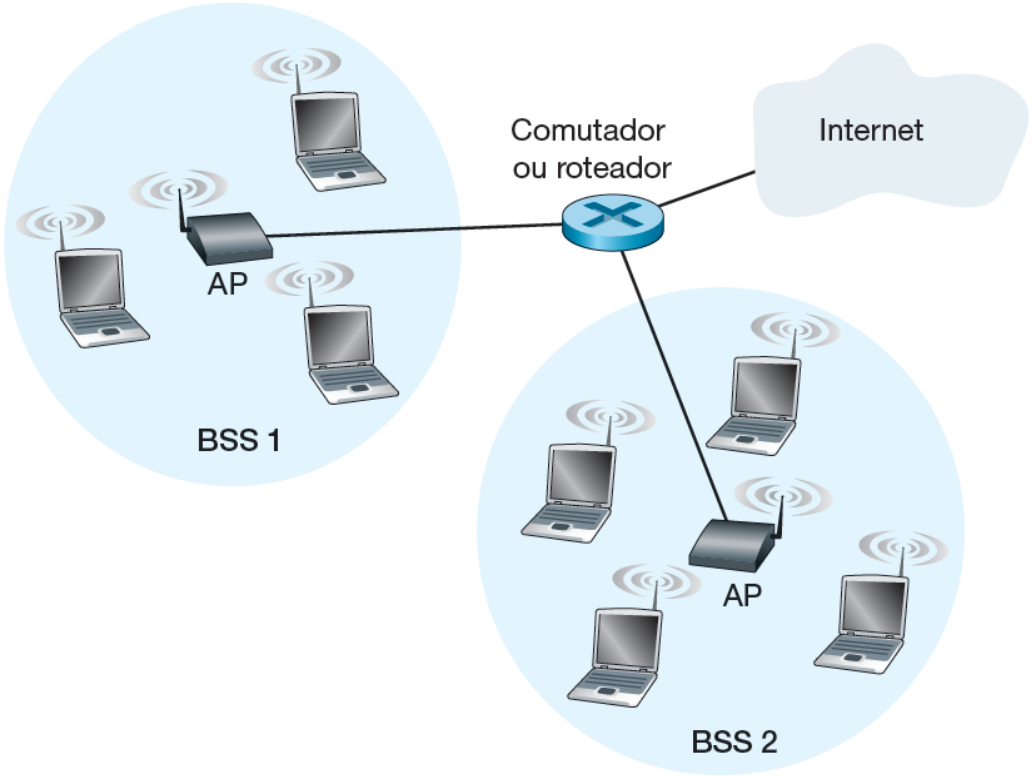


Atenuação de Sinal:

- B, A ouvir um ao outro
- B, C ouvir um ao outro
- A, C não conseguem ouvir um ao outro, interferindo em B.

A arquitetura 802.11

- A arquitetura de LAN IEEE 802.11



Canais e associação

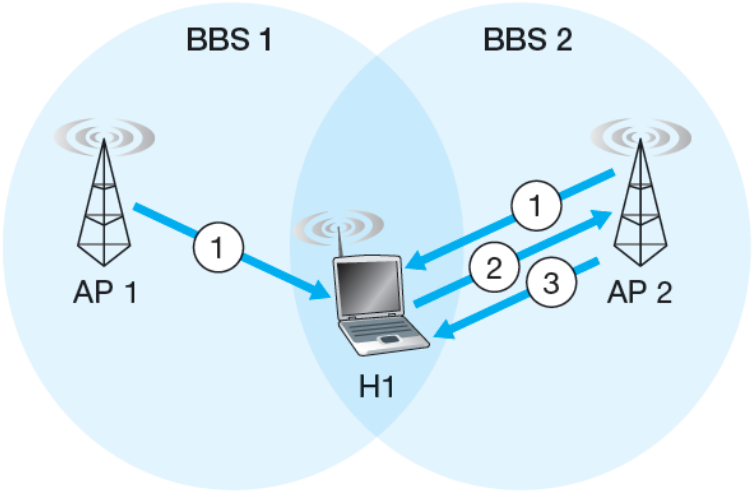
- Em 802.11, cada estação sem fio precisa se associar com um AP antes de poder enviar ou receber dados da camada de rede.
- Ao instalar um AP, um administrador de rede designa ao ponto de acesso um **Identificador de Conjunto de Serviços** composto de uma ou duas palavras.
- Ele também deve designar um número de canal ao AP.
- Uma **selva de Wi-Fis** é qualquer localização física na qual uma estação sem fio recebe um sinal suficientemente forte de dois ou mais APs.

Canais e associação

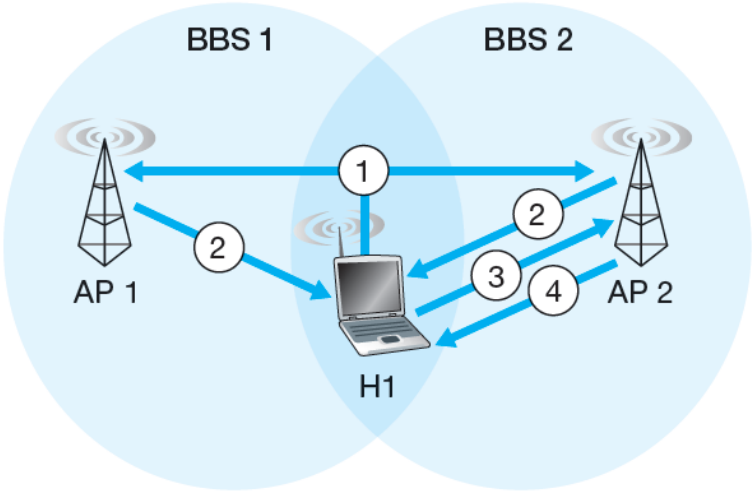
- Em geral, o hospedeiro escolhe o AP cujo quadro de sinalização é recebido com a intensidade de sinal mais alta.
- O processo de varrer canais e ouvir quadros de sinalização é conhecido como **varredura passiva**.
- Um hospedeiro sem fio pode também realizar uma **varredura ativa**, transmitindo um quadro de investigação que será recebido por todos os APs dentro de uma faixa do hospedeiro sem fio.

Canais e associação

- Varredura passiva e ativa para pontos de acesso

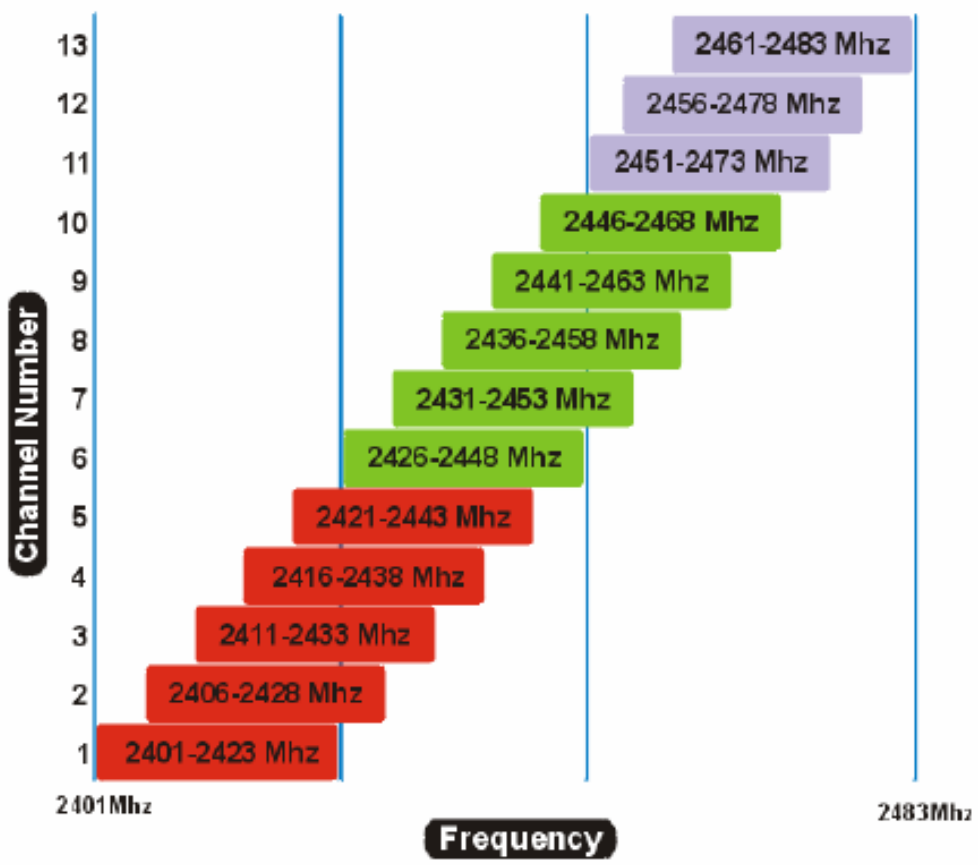


a. Varredura passiva
1. Quadros de sinalização enviados dos Aplicações
2. Quadro de Solicitação de Associação enviado: H1 para AP selecionado
3. Quadro de Resposta de Associação enviado: AP selecionado para H1



a. Varredura ativa
1. Difusão do quadro de Solicitação de Investigação de H1
2. Quadro de Resposta de Investigações enviado das Aplicações
3. Quadro de Solicitação de Associação enviado: H1 para AP selecionado
4. Quadro de Resposta de Associação enviado: AP selecionado para H1

Canais e associação



Source: www.draytek.co.uk/support

Métodos de acesso ao meio

DCF (Distributed Coordination Function)

- As estações competem pelo entre si pelo meio
- Uso de CSMA/CA

PCF (Point Coordination Function)

- É Opcional;
- AP escuta estações em turnos para verificar se há frames;
- Elimina Colisões;
- Coexiste com DCF em uma rede;

Métodos de acesso ao meio

- **CSMA/CA**
  - Dispositivo “escuta” o meio e, se o meio estiver livre por tempo determinado (DIFS) ; transmite; senão backoff
  - Tempo de backoff é randômico, para evitar colisões
  - Uso de ACK para verificar entrega
- **CSMA/CA com RTS/CTS - Request to Send and Clear to Send (RTS/CTS) (opcional)**
  - Mecanismo de reserva para evitar terminal escondido
- **Interframe Spaces (IFS)**
  - SIFS (Short) – alta prioridade: ACK, RTS, polling (resposta)
  - PIFS (PCF) – prioridade média, uso com PCF, polling (req)
  - DIFS (DCF) – prioridade mais baixa
  - EIFS (Extended) – retransmissão de quadros com erro

O protocolo MAC 802.11

- Inspirados pelo enorme sucesso da Ethernet e seu protocolo de acesso aleatório, os projetistas do 802.11 escolheram um protocolo de acesso aleatório para as LANs sem fio 802.11.

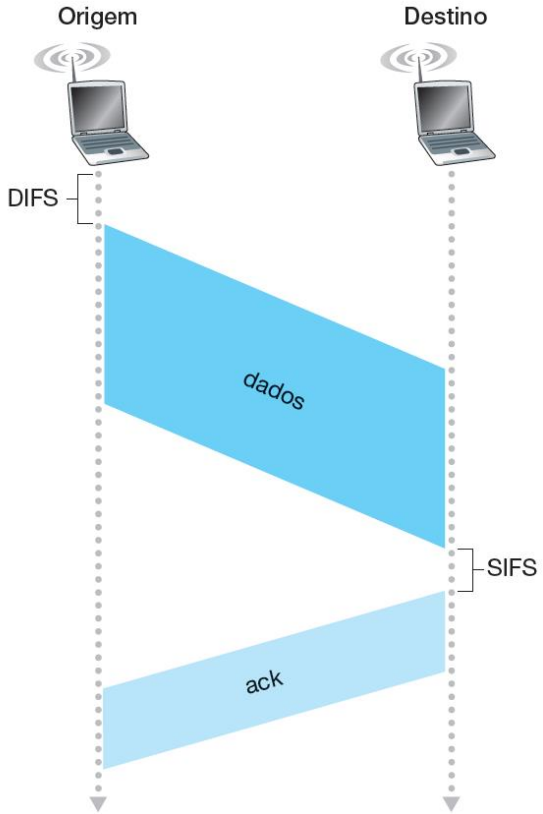
- Esse protocolo de acesso aleatório é denominado **CSMA com prevenção de colisão** ou, mais sucintamente, **CSMA/CA**.

- Em vez de usar detecção de colisão, o 802.11 usa técnicas de prevenção de colisão.

- Usa um esquema de reconhecimento/retransmissão (ARQ) de camada de enlace.

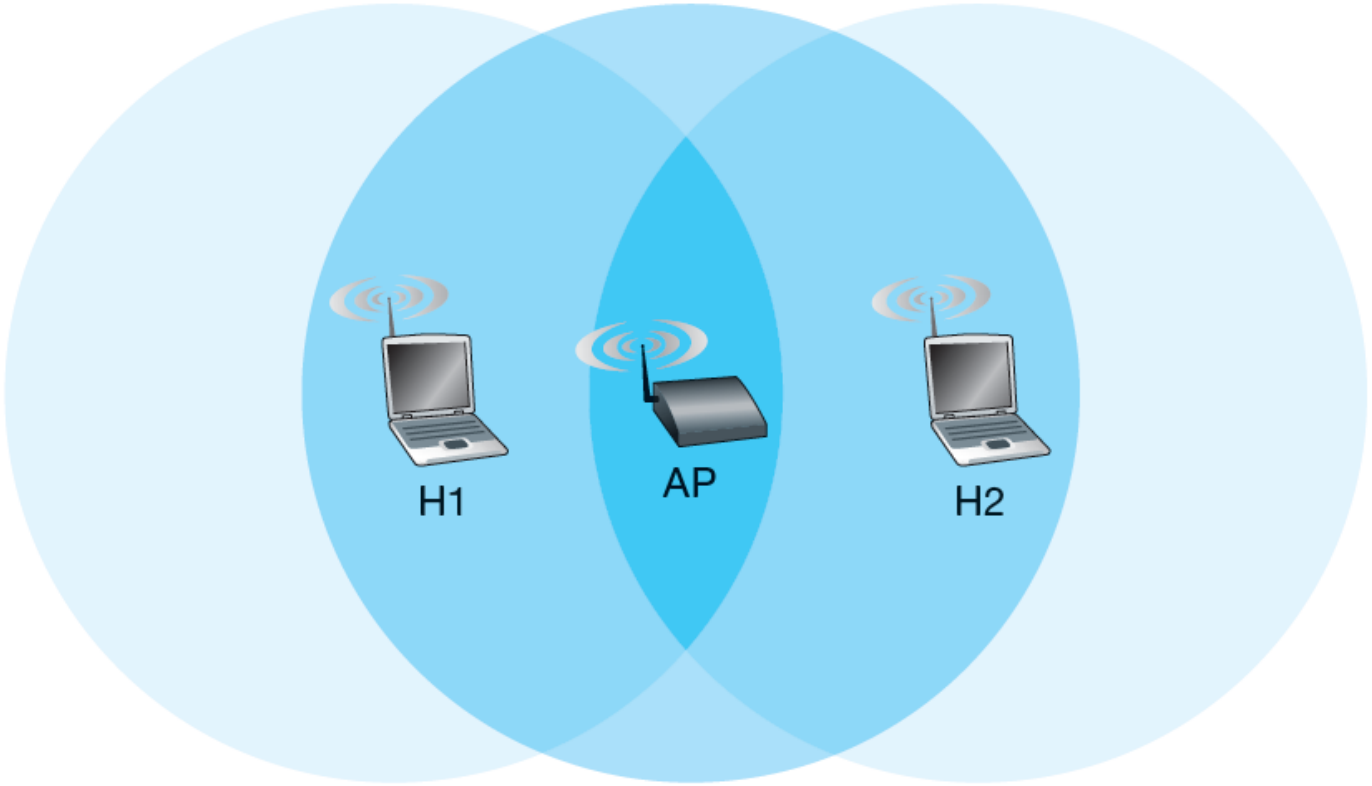
O protocolo MAC 802.11

- 802.11 usa reconhecimentos da camada de enlace



Tratando de terminais ocultos: RTS e CTS

- Exemplo de terminal oculto: H1 está oculto de H2, e vice-versa



Tratando de terminais ocultos: RTS e CTS

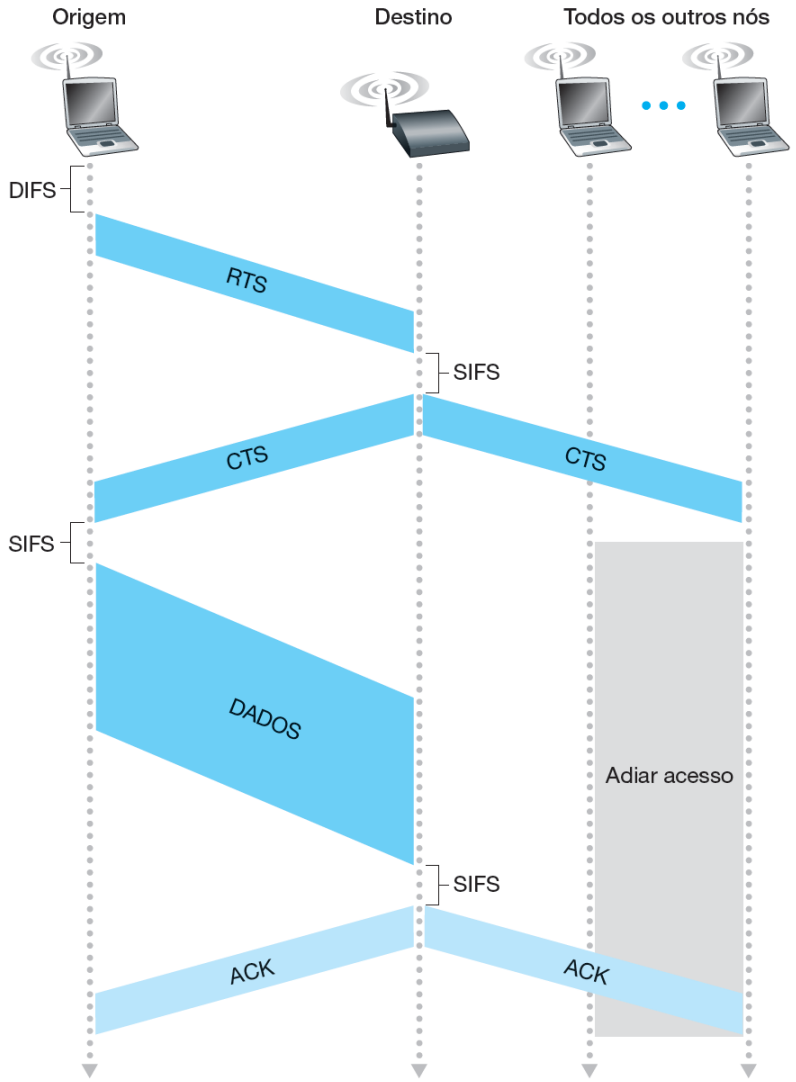
- O protocolo IEEE 802.11 permite que uma estação utilize um quadro de controle **RTS** curto e um quadro de controle **CTS** curto para reservar acesso ao canal.

- A utilização dos quadros RTS e CTS pode melhorar o desempenho de dois modos importantes:

1. O problema da estação oculta é atenuado.

2. Desde que os quadros RTS e CTS sejam corretamente transmitidos, os quadros DATA e ACK subsequentes deverão ser transmitidos sem colisões.

Tratando de terminais ocultos: RTS e CTS



- Prevenção de colisão usando os quadros RTS e CTS.

O quadro IEEE 802.11

- O quadro 802.11

Quadro (os números indicam o comprimento do campo em bytes):

2	2	6	6	6	2	6	0-2312	4
Controle de quadro	Duração	Endereço 1	Endereço 2	Endereço 3	Controle de sequência	Endereço 4	Carga útil	CRC

Detalhamento do campo de controle do quadro (os números indicam o comprimento do campo em bits):

2	2	4	1	1	1	1	1	1	1	1
Versão do protocolo	Tipo	Subtipo	Para o AP	Do AP	Mais frag	Nova tentativa	Ger. de energia	Mais dados	WEP	Reser-vado

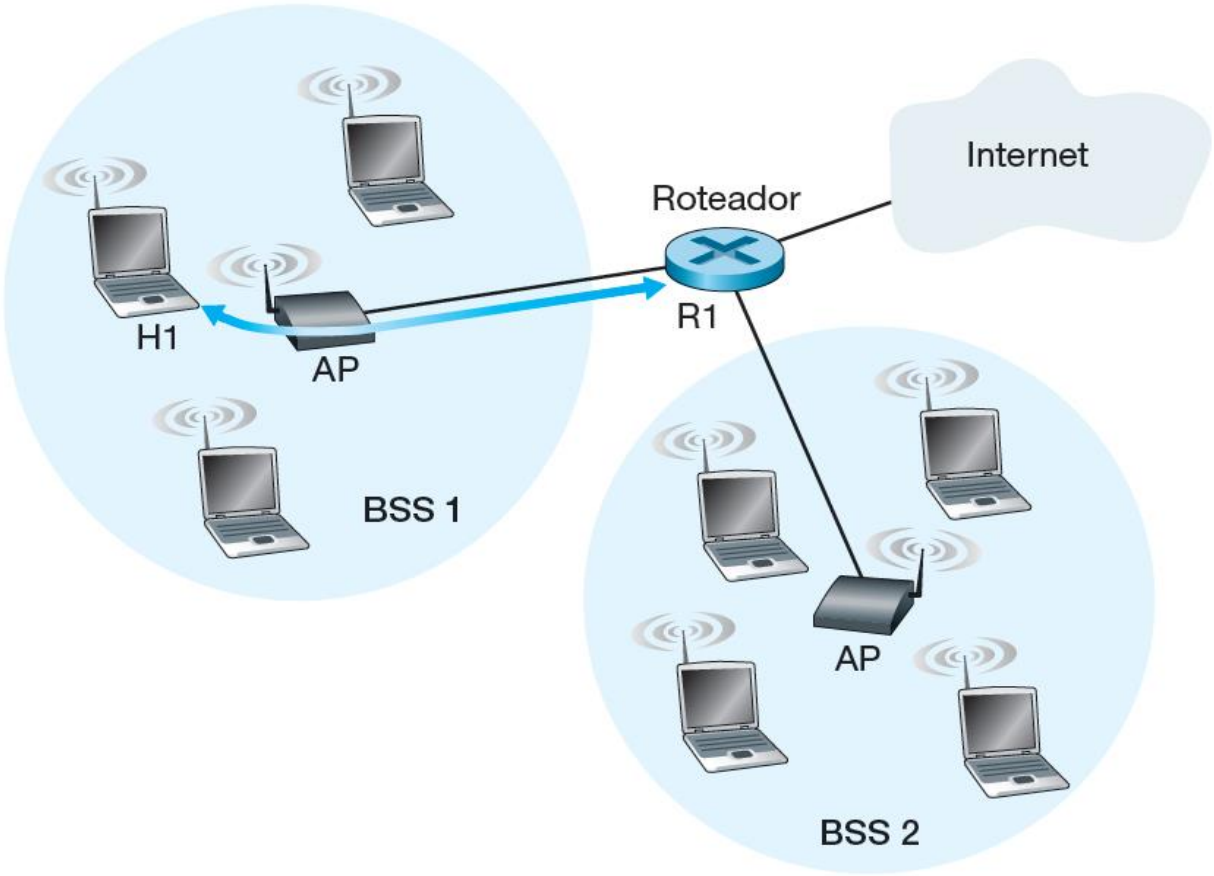
O quadro IEEE 802.11

- No coração do quadro está a carga útil, que consiste, tipicamente, em um datagrama IP ou em um pacote ARP.

- Talvez a diferença mais marcante no quadro 802.11 é que ele tem quatro campos de endereço e cada um pode conter um endereço MAC de 6 bytes.

- A figura a seguir mostra a utilização de campos de endereço em quadros 802.11: movendo um quadro entre H1 e R1.

O quadro IEEE 802.11



O quadro IEEE 802.11

- Os campos *tipo* e *subtipo* são usados para distinguir os quadros de associação, RTS, CTS, ACK e de dados.
- Os campos *de* e *para* são usados para definir os significados dos diferentes campos de endereço.
- O campo *WEP* (*Wireless Equivalent Privacy*) indica se está sendo ou não utilizada criptografia.

Recursos avançados em 802.11

Adaptação da taxa 802.11

- Algumas execuções de 802.11 possuem uma capacidade de adaptação de taxa que seleciona, de maneira adaptável, a técnica de modulação da camada física sobreposta a ser usada com base em características atuais ou recentes do canal.

- A adaptação da taxa 802.11 e o controle de congestionamento TCP são semelhantes à criança: está sempre exigindo mais e mais de seus pais até eles por fim dizerem “Chega!” e a criança desistir.

Recursos avançados em 802.11

Gerenciamento de energia

- O padrão 802.11 provê capacidades de gerenciamento de energia, permitindo que os nós 802.11 minimizem o tempo de suas funções de:
- percepção,
- transmissão e recebimento, e
- outros circuitos necessários para “funcionar”.

Redes pessoais: Bluetooth e Zigbee

- As camadas de enlace e física do 802.15.1 são baseadas na especificação do **Bluetooth** anterior para redes pessoais.
- Redes 802.15.1 operam na faixa de rádio não licenciada de 2,4 GHz em modo TDM, com intervalos de tempo de 625 μs.
- Redes 802.15.1 são redes *ad hoc*.
- Dispositivos 802.15.1 são primeiro organizados em uma picorrede (piconet: pequena rede) de até oito dispositivos ativos.

Redes pessoais: Bluetooth e Zigbee

- **Zigbee** é voltada para aplicações de menos potência, menor taxa de dados e menor ciclo de trabalho do que Bluetooth.
- Zigbee define taxas de canal de 20, 40, 100 e 250 Kbits/s, dependendo da frequência do canal.
- Os nós em uma rede Zigbee podem ser de dois tipos.
- Os chamados “dispositivos de função reduzida” operam como escravos controlados por um único “dispositivo de função completa”, assim como dispositivos Bluetooth escravos.

Segurança WIFI

- Riscos maiores de invasão
  - Não é necessário acesso físico à rede para invadir
- Má configuração de Aps
  - Configuração padrão geralmente é insegura – sem criptografia e com SSID de rede padrão
- Clientes/Aps não autorizados
  - Não há autenticação e DHCP concede IP a qualquer um
- Interceptação de tráfego
  - Sniffer sem necessidade de acesso físico à rede
  - Vários protocolos com senha em texto simples (smtp; pop; ftp)

Segurança WIFI / WEP

- WEP (Wired Equivalency Privacy)
  - Príncipio: chaves simétricas distribuídas
  - Proposta: proteção contra interceptação (autenticidade; confidencialidade e integridade)
- Autenticação na camada de enlace
  - não é fim-a-fim
- Modos
  - Open system – modo default
  - Shared key – chave wep para mecanismo challeng-response
- Chave RC4 – 40 bits

Segurança WIFI / WEP Restrições

- Somente o cliente é autenticado
  - Aps falsos podem enganar os clientes
- Integridade dos dados não é garantida
  - CRC32 é função linear e o conteúdo da mensagem pode ser alterado sem conhecimento prévio da chave Wep
- RC4 possui falhas na geração
  - Geração da sequência quando é conhecida uma parte da chave
- Ferramentas de domínio público fazem descoberta de chaves Wep
  - Airsnort
  - WEPCrack

Segurança WIFI / WPA

- Wi-Fi Protected Access
- Especificado por um grupo de fabricantes chamado “Wi-Fi Alliance”
- Criptografia: TKIP
  - Temporal Key Integrity Protocol – chaves Wep mudam de tempos em tempos
  - Chave possui 128 bits
  - Chaves de sessão dinâmicas: Por usuário, por sessão ou até por pacote
- Autenticação
  - 802.1x e EAP (usuários corporativos)
  - Passphrase (Usuário doméstico)

Segurança WIFI / WPA2

- WPA baseava-se em um draft da norma 802.11i
- Quando a norma foi finalizada, criou algumas melhorias e foi chamada de WPA2
  - Também conhecida por Robust Security Network (RSN)
- Melhorias
  - Mudança na criptografia de TKIP para AES
  - Abandono do RC4, com uso de CCMP
- Requer mais mudanças que o WPA no HW e SW dos equipamentos